UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/710,350	07/02/2004	Andre KRAMER	2006579-0444	4349

69665 7590 10/04/2007

CHOATE, HALL & STEWART / CITRIX SYSTEMS, INC.
TWO INTERNATIONAL PLACE
BOSTON, MA 02110

EXAMINER	
LEMMA, SAMSON B	
ART UNIT	**PAPER NUMBER**
2132	

MAIL DATE	DELIVERY MODE
10/04/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/710,350	KRAMER, ANDRE	
	Examiner	Art Unit	
	Samson B. Lemma	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *02 July 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-29* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-29* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *01/06/2006*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This is in reply to application filed on July 2nd 2004. Claims 1-29 are pending of which 4 of them are independent claims, namely claims 1, 15, 26 and 29. All **claims (1-29)** have been examined.

Priority

2. This application does not claim priority of an application. Therefore, the effective filling data for the subject matter defined in the pending claims of this application is **07/02/2004.**

Claim Objections

3. Dependent claim 27 is objected to because of the following informalities: dependent claim 27 depends on itself, for the sake of examination it is assumed to depend on independent claim 26.

Appropriate correction is required.

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

5. **Claims 1-29** are rejected under 35 U.S.C. 102(b) as being anticipated by **Publication, IBM Technical Disclosure Bulletin, title, "Administrative Role Configuration with Control Lists" TDB-ACC-NO: NB9112110** (hereinafter referred as IBM) (Publication date: December 1, 1991)(See Reference U)

Examiner has pointed out particular references contained in the prior arts of record in the body of this action for the convenience of the applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may apply as well. Applicant should consider the entire prior art as applicable as to the limitations of the claims. It is respectfully requested from the applicant, in preparing the response, to consider fully the entire references as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior arts or disclosed by the examiner

6. **As per independent claims 1 and 26 IBM discloses a method for providing secure access to applications** *[Page 3, lines 32-34]* **(***This is extended by means of a Privilege Control List mechanism, which works in much the same way as the Access Control List mechanism described in the following article)*

the method comprising the steps of:

- **Receiving a request from a user to execute an application** *[Page 4, lines 19-20 and page 4, lines 16-17[On page 4, lines 19-20, see "the command is executed by direct user invocation by shell script or via system call or subroutine."" and on page 4, lines 16-17, see "any method executing the command");*

- **Determining a minimal set of computing privileges necessary for the user to use the requested application** *[Page 3, lines 29-34] (The disclosed mechanism works in conjunction with* ***the least privilege mechanism*** *described in (*), which describes mechanism for associating a set of discrete privileges with a file. This is extended by means of a Privilege Control List mechanism, which works in much the same way as the Access Control List mechanism described in the following article.)*; **and**

- **Invoking an execution environment for the user having the determined set of privileges** *[Page 4, lines 16-18 and page 4, lines 18-21] (On page 4, lines 16-18, the following has been disclosed. "any method of executing the command will 'work' - that is, the* ***invoker will acquire the correct privileges.****" Furthermore on page 4, lines 18-21, the following has been disclosed. "this method allows privilege to be acquired whether the command is executed by* ***direct user invocation,*** *by shell script or via system call or subroutine.")*

7. **As per independent claims 15 & 29, and dependent claim 16 IBM discloses an application server system providing secure access to hosted applications,** *[Page 3, lines 32-34] (On page 3, lines 32-34, the following for instance has been disclosed. This is extended by means of a Privilege Control List mechanism, which works in much the same way as the Access Control List mechanism described in the following article and this meets the limitation recited as "providing secure access to hosted application)* ***the system comprising:***

- **A policy based decision system receiving a request from a user to execute an application** *[On page 3, lines 32-34, the following for instance has been disclosed. This is extended by means of a Privilege Control List mechanism, which works in much the same way as the Access Control List mechanism described in the following article and this meets the limitation of a policy based decision system. Furthermore, on page 3, lines 34-page 4, line 1, the following has been disclosed. A Privilege Control List (PCL) consists of an unordered set of Privilege Control Entries. Each entry consists of a list of typed identifiers and a set of privileges. The list of typed identifiers defines the circumstances under which the privileges will be granted and this also meets the limitation recited as "***A policy based decision system***") receiving a request from a user to execute an application* *(Page 3, lines 32-34, Page 4, lines 19-20 and page 4, lines 16-*

17][On page 4, lines 19-20, see "the command is executed by direct user invocation by shell script or via system call or subroutine." and on page 4, lines 16-17, see "any method executing the command"); **and determining a minimal set of privileges required by the user to execute the application** *[Page 3, lines 29-34] (The disclosed mechanism works in conjunction with the least privilege mechanism described in (*), which describes mechanism for associating a set of discrete privileges with a file. This is extended by means of a Privilege Control List mechanism, which works in much the same way as the Access Control List mechanism described in the following article.)*;

- **An account administration service in communication with said policy based decision system, the account administration service invoking an execution environment for the user having the determined set of privileges;** [See page 4, lines 12-23] (On page 4, lines 12-23, the following has been disclosed. "*Since the commands themselves do not enforce policy, the* ***administrator who controls privilege assignment is free to configure the system roles in whatever manner is appropriate for the local system"****, and this meets "the account administration service". Furthermore the following has been disclosed- "This mechanism is also compatible with existing practice. Because the privilege is associated directly with the program file, any method of executing the command will 'work' - that is, the invoker will acquire the correct privileges. Unlike the second mechanism described above, this method allows privilege to be acquired whether the command is executed by direct user invocation, by shell script or via system call or subroutine. - Lastly, this mechanism allows privilege to be granted based on arbitrary combinations of identifiers, thus increasing the flexibility with which the system privilege control policy can be defined" and this meets the limitation "an account administration service in communication with said policy based decision system, the account*

administration service invoking an execution environment for the user having the determined set of privileges".) and

A connection manager in communication with said policy based decision system *[See again page 4, lines 19-20 and 4, lines 16-17 "the entity/interface receiving client's request/execution command meet the limitation of connection manager and this interfaces between the user and the Privilege Control List system/policy based decision system"],* **said connection manager receiving from a client system an RDP request by the user to execute the application** *[Page 4, lines 19-20 and page 4, lines 16-17][On page 4, lines 19-20, see "the command is executed by direct user invocation by shell script or via system call or subroutine."" and on page 4, lines 16-17, see "any method executing the command");* **and transmitting to said policy based decision system an identification of said user and an identification of said application.** *[See on page 3, lines 32-page 4, line 1 and page 4, lines 16-23] (On page 3, lines 32-page 4, the following has been disclosed. This is extended by means of a Privilege Control List mechanism, which works in much the same way as the Access Control List mechanism described in the following article. A Privilege Control List (PCL) consists of an unordered set of Privilege Control Entries. Each entry consists of a list of typed identifiers and a set of privileges. The list of typed identifiers defines the circumstances under which the privileges will be granted. This meets the limitation recited as "policy based decision system based on identification of said user". Furthermore, the following has been stated. "This mechanism is also compatible with existing practice. Because the privilege is associated directly with the program file and this meets the limitation recited as "policy based decision system based on identification of said application", any method of executing the command will 'work' - that is, the invoker will acquire the correct privileges. Unlike the second mechanism described above, this method allows privilege to be*

acquired whether the command is executed by direct user invocation, by shell script or via system call or subroutine. - Lastly, this mechanism allows privilege to be granted based on arbitrary combinations of identifiers, thus increasing the flexibility with which the system privilege control policy can be defined

8. **As per dependent claims 2-3 and 17-18IBM discloses a method as applied to claims above. Furthermore, IBM discloses the method, comprising the further step of: returning an identifier for the execution environment to the requesting user.** *[Page 4, lines 18-23 and page 3, lines 34-page 4, lines 4] (For instance on page 4, lines 18-23 the following has been disclosed. "This mechanism allows privilege to be granted based on* ***arbitrary combinations of identifiers****, thus increasing the flexibility with which the system privilege control policy can be defined." Furthermore on page 3, lines 34-page 4, lines 4, the following has been disclosed. "A Privilege Control List (PCL) consists of an unordered set of Privilege Control Entries. Each entry consists of a list of typed identifiers and a set of privileges. The list of typed identifiers defines the circumstances under which the privileges will be granted, and the format of the data structures permits extension to arbitrary types of identifiers")*

9. **As per dependent claim 4 IBM discloses a method as applied to claims above. Furthermore, IBM discloses the method, wherein step (a) comprises receiving an HTTP-based request from a user to execute an application.** *[Page 4, lines 19-20 and page 4, lines 16-17[On page 4, lines 19-20, see "the command is executed by direct user invocation by shell script or via system call or subroutine."" and on page 4, lines 16-17, see "any method executing the command");*

10. **As per dependent claims 5-8, 20-25 and 27-28 IBM discloses a method as applied to claims above. Furthermore, IBM discloses the method, wherein step (b) comprises accessing a policy-based decision system to determine a minimal set of computing privileges necessary for the user to use the requested application.**

[Page 3, lines 29-34 and page 3, lines 35- page 4, line 4] (The disclosed mechanism works in conjunction with ***the least privilege mechanism*** *described in (*), which describes mechanism for associating a set of discrete privileges with a file. This is extended by means of a Privilege Control List mechanism, which works in much the same way as the Access Control List mechanism described in the following article.)*

11. As per dependent claims 9 and 19 IBM discloses a method as applied to claims above. Furthermore, IBM discloses the method, further comprises determining a minimal set of computing privileges necessary for the user to use the requested application based, at least in part, on a role assigned to the user. *[page 4, lines 12-14* **]***[See at least the title, "administrative role configuration" with privilege control lists and see on page 4, lines 12-14, "Since the commands themselves do not enforce policy, the administrator who controls privilege assignment is free to configure the system roles in whatever manner is appropriate for the local system" and on page Page 3, lines 29-34 and page 3, lines 35- page 4, line 4, see "the least privilege mechanism")*

12. As per dependent claims 10-13 IBM discloses a method as applied to claims above. Furthermore, IBM discloses the method, wherein step (c) further comprises creating an execution environment for the user having the determined set of privileges. [*Page 4, lines 16-18 and page 4, lines 18-21] (On page 4, lines 16-18, the following has been disclosed. "any method of executing the command will 'work' - that is, the* ***invoker will acquire the correct privileges.*** *" Furthermore on page 4, lines 18-21, the following has been disclosed. "this method allows privilege to be acquired whether the command is executed by* ***direct user invocation,*** *by shell script or via system call or subroutine.")*

13. As per dependent claims 14 IBM discloses a method as applied to claims above. Furthermore, IBM discloses the method, further comprising the steps of

initiating a connection with a client system associated with the user. [*Page 4, lines 16-18 and page 4, lines 18-21] (See for instance, command is executed by* ***direct user invocation)***

Conclusion

14. *The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.(See PTO-Form 892).*

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Samson B Lemma whose telephone number is 571-272-3806. The examiner can normally be reached on Monday-Friday (8:00 am---4: 30 pm).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, BARRON JR GILBERTO can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 703-873-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

SAMSON LEMMA

S.L. (S.L.)

09/10/2007

GILBERTO BARRON JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100